

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-122976

(P2000-122976A)

(43) 公開日 平成12年4月28日 (2000.4.28)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 G 5 B 0 5 8
G 0 6 K 17/00		G 0 6 K 17/00	U 5 B 0 8 5
G 0 8 B 25/04		G 0 8 B 25/04	E 5 C 0 8 7
H 0 4 B 1/59		H 0 4 B 1/59	5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 E

審査請求 未請求 請求項の数 4 O L (全 9 頁) 最終頁に続く

(21) 出願番号 特願平10-294255

(22) 出願日 平成10年10月15日 (1998.10.15)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 明星 俊彦

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

(74) 代理人 100087446

弁理士 川久保 新一

Fターム(参考) 5B058 CA15 KA31 KA33 YA11 YA20

5B085 AE11

5C087 AA02 BB20 BB46 DD03 DD06

DD14 DD43 EE06 EE07 EE10

FF19 GG06 GG10 GG17

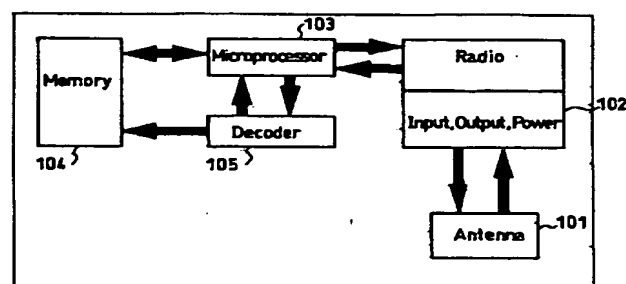
5J104 AA07 KA02 NA05 PA01

(54) 【発明の名称】 セキュリティシステム

(57) 【要約】

【課題】 データキャリアと主装置とから構成されるデータキャリアシステムを利用して各種装置の動作起動のセキュリティを管理することができるセキュリティシステムを提供する。

【解決手段】 コンピュータの電源立ち上げ時やプログラム起動時、自動車のエンジン起動時等、所望の動作起動時にのみ主装置からの照合電波の送出を行う。そして、データキャリアから返送された照合データを予め主装置に登録されたデータと照合し、この照合において一致した場合に起動動作を継続する。また、照合において不一致の場合、起動動作を停止させる。また、最終使用履歴を更新してデータキャリアに通知して保存させ、上述したデータ照合時に最終使用履歴の照合を行い、不一致の場合、ユーザに警告する。



1

【特許請求の範囲】

【請求項1】 動作起動をかけることにより、所望の動作を行う装置のセキュリティシステムにおいて、データを電波により送受信する主装置と、前記電波を受信した後、この電波のエネルギーを利用してデータ通信を行う非接触型データキャリア装置とを有し、前記動作起動時に、起動要求ユーザが使用権をもっていることを確認するために、前記主装置より登録ユーザ照合電波を送出する照合電波送出手段と、前記登録ユーザ照合電波を受けたデータキャリア装置において、設定された照合データを返送する照合データ返送手段と、前記主装置において、データキャリア装置の返送手段によって返送された照合データと予め登録されたユーザ情報とを照合するユーザ照合手段と、前記照合の結果、ユーザが不一致の場合、起動動作を禁止する禁止手段と、を有することを特徴とするセキュリティシステム。

【請求項2】 請求項1において、前記主装置は、個別ユーザ情報を登録する個別ユーザ情報登録手段と、この登録された個別ユーザ情報を送出する個別ユーザ情報送出手段とを有し、前記データキャリア装置は、前記個別ユーザ情報送出手段より送出された個別ユーザ情報を記憶する記憶手段を有し、前記主装置は、前記データキャリア装置側で個別ユーザ情報が正しく記憶されたことを確認する確認手段と、前記個別ユーザ情報の登録失敗時に再度登録動作を繰り返す再登録手段とを有する、ことを特徴とするセキュリティシステム。

【請求項3】 請求項1において、前記ユーザ照合手段は、個別ユーザ情報に加え、最終使用履歴の照合を行う使用履歴照合手段と、最終使用履歴の更新を行う使用履歴更新手段と、前記使用履歴照合において不一致の場合、ユーザに警告する警告手段と、を有することを特徴とするセキュリティシステム。

【請求項4】 請求項1において、前記主装置は、送出する電波に主装置の識別コードを付加する識別コード付加手段を有し、前記データキャリア装置は、前記主装置の識別コードに応じて複数の個別ユーザ情報を登録する登録手段と、主装置からの照合信号を受けた場合に、主装置の識別コードに応じて登録された個別ユーザ情報を選択して送出する個別ユーザ情報送出手段とを有する、ことを特徴とするセキュリティシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、動作起動をかけることにより、所望の動作を行う装置のセキュリティシ

2

テムに関する。

【0002】

【従来の技術】 従来、コンピュータのセキュリティとしては、所望の動作を行うにあたりユーザが予め登録したパスワード等によりセキュリティをかけており、またネットワークに接続されている場合、サーバ等において、予め使用権を与えるユーザを登録する等の手段により、セキュリティをかけている。

【0003】 また、自動車においては、盗難防止のために鍵が一定時間以上装着され、なおかつエンジンの始動がなされない場合には、エンジンの始動を禁止し、特殊な鍵をセキュリティシステムに接続し、個別コードを読み出させることにより、この機能を解除するセキュリティシステム等が用いられている。

【0004】 一方、データを電波により送受信する装置（以下主装置という）と、該電波を受信した後、この電波のエネルギーを利用してデータ通信を行う非接触型装置（以下データキャリア装置という）により構成されるデータキャリアシステム（たとえば自動入退室管理システム）が知られている。

【0005】 そして、このようなデータキャリアシステムにおいては、主装置では常に電波を送出し、そのそばを通るデータキャリア装置をもつユーザは、特に意識することなく相手に存在を知らしめる（または情報交換）を行うことができる構成となっている。

【0006】

【発明が解決しようとする課題】 しかしながら、前記従来例におけるコンピュータのセキュリティでは、パスワードを何らかの理由により第三者が知った場合、容易にコンピュータを操作することが可能となり、さらにこの不正使用されたコンピュータを利用することで、サーバ等へのアクセスも容易に行え、コンピュータデータに対するセキュリティは保たれないといった問題点がある。

【0007】 また、上述した自動車の例においては、セキュリティシステムが稼動した場合、ユーザが特殊な鍵を接続して解除する必要がある、面倒であるといった問題点がある。

【0008】 また、上述した従来のデータキャリアシステムでは、常に主装置より電波の送出が行われることから、ラップトップコンピュータや自動車のようなバッテリー駆動を行う装置においては、電力消費量に問題があった。

【0009】 そこで本発明は、データキャリアシステムを利用して各種装置の動作起動のセキュリティを管理することができ、かつ、データキャリアシステムの節電を図ることができるセキュリティシステムを提供することを目的とする。

【0010】

【課題を解決するための手段】 本発明は、コンピュータの電源立ち上げ時やプログラム起動時、自動車のエンジ

10

20

30

40

50

3

ン起動時等、所望の動作起動時にのみ主装置からの照合電波の送出を行う照合電波送出手段と、返送された照合データを登録されたデータと照らし合わせる照合手段と、この照合において一致した場合に起動動作を継続する手段、および、最終使用履歴を更新してデータキャリア装置に通知保存する通知保存手段と、上述した照合において不一致の場合、起動動作を停止させる禁止手段を有する。

【0011】したがって、例えばコンピュータのセキュリティに用いる場合、データキャリア装置に個別ユーザ情報および最終使用履歴を保存する保存手段と、照合要求があった場合、蓄積されたデータを主装置に返送する返送手段を有することにより、OS等のもつパスワードによる保護に加え、使用者を登録されたデータキャリア装置をもつユーザのみに特定でき、より信頼性の高いセキュリティが確保できる。

【0012】また、さらに最終使用履歴を主装置およびデータキャリア装置でそれぞれ有し、照合時に互いのデータに違いがないことを確認する確認手段を有することにより、仮にデータキャリア装置を不正に複製された場合においても、ユーザがコンピュータの不正使用されたことを知ることが可能となり、容易に個別ユーザ情報の変更等による対策が行える。

【0013】また、自動車のセキュリティに用いた場合においては、常にエンジン始動時に照合動作が行われることから、ユーザは意識することなく常に盗難防止機能がかけられる。

【0014】さらに、主装置の識別コードを伝送データに組み込むことで、入退室管理システム等、複数のシステムを1つのデータキャリア装置で共用することが可能となり、ユーザは意識することなく複数のシステムを使用できる。

【0015】また、以上のような構成を用いることにより、システム全体の消費電力を大幅に削減することが可能となり、バッテリー駆動の機器にも容易に用いることができる。

【0016】

【発明の実施の形態および実施例】 {第1実施例} 図1は、本発明の実施例におけるデータキャリア装置の内部構成を示すブロック図である。

【0017】また、図2(a)は、本実施例において主装置から送られる総合電波内のデータフォーマットを示す説明図であり、図2(b)は、本実施例におけるデータキャリア装置内のメモリ配置フォーマットを示す説明図である。

【0018】また、図3は、本実施例によるシステムを構成する機器の外観を示す説明図である。

【0019】さらに、図4は、本実施例の主装置における個別ユーザデータ登録動作の概略を示すフローチャートであり、図5は、本実施例の主装置における照合動作

4

の概略を示すフローチャートである。

【0020】図1において、アンテナ101は、主装置から伝送される電波を受信するためのものであり、無線部102は、アンテナ101を介してデータの送受信を行うとともに、受信電波から電力を生成するものである。プロセッサ103は、デコーダ105を介して受信データを解析し、要求に応じてメモリ104への書き込み読み出し動作等を行うものであり、メモリ104は、個別ユーザ情報等を記憶するものである。

10 【0021】図2(a)(b)において、制御信号部201は送受信されるデータの種類、読み出し書き込み指示、新規登録データ更新表示等の情報を示すためのものであり、主装置識別コード部202は、主装置を識別するためのものである。個別ユーザ情報部203は、個別ユーザを識別するためのものである。また、メモリエリア204は、データキャリア装置内のメモリ104に割り当てられた主装置から登録されるデータを格納するためのエリアである。

20 【0022】図3において、主装置301は、本実施の各種処理を実行するコンピュータ等であり、アンテナ302は、主装置301から電波を送出するものである。また、データキャリア装置303は、例えば身分証明書のような形態を有し、上述した個別ユーザ情報が記憶されている。

【0023】以下、本実施例における具体的な動作についてフローチャートに基づき説明する。

【0024】まず本実施例の主装置301において、使用ユーザを特定する場合、図4に示す登録動作を行う。なお、図4は動作の概略を示すものであり、詳細は省略している。

30 【0025】この登録動作としては、まずユーザは個別ユーザ情報としてユニークな番号文字等をコンピュータのパスワード登録手順と同様にして入力し(S1)、その後、主装置301からの電波送出指示を行う。この指示を受けた主装置301は新規登録、登録要求を示す値を制御信号部201に組み込むとともに、主装置識別コードを主装置識別コード部202に組み込み、このデータをアンテナ302を介して送出した後(S2)、データキャリア303からの登録応答受信検出を待機する(S3)。

40 【0026】このとき、個別ユーザ情報を記憶させるべきデータキャリア装置303が通信圏内にない場合は(S4)、その旨をユーザに通知し、再度電波送信指示を待機する。

【0027】一方、主装置301から登録要求電波をアンテナ101から受信したデータキャリア装置303は無線部102より電力および受信信号を得た後、プロセッサ部103によりその受信信号解析を行う。そして、新規登録要求信号であると判断した場合、メモリ104のエリア(たとえば204)が空きであることを確認し

50

5

た後に主装置301に対して登録応答信号を送出する。

【0028】この登録応答を受けた主装置301は(S3)、次いで情報登録指示を示す信号を制御信号部201に書き込み、設定された個別ユーザ情報を個別ユーザ情報部203に書き込んだ信号送出を前述と同様の手順により行う。

【0029】伝送された信号を受信したデータキャリア装置303では、やはり前述と同様の手順によりプロセッサ部103によりデータ解析を行った後、メモリ主装置識別コード部201と個別ユーザデータ部203のデータを書き込む。

【0030】個別ユーザ情報を送出した主装置301は、次いで情報登録確認のためにユーザ照合を示す信号を制御信号部201に書き込んだ信号を送出した後(S5)、応答を待機する。

【0031】また、この信号を受信したデータキャリア装置303は、やはり前述と同様の手順により解析を行った後、メモリ104より主装置識別コードの一致するエリアに登録されている個別ユーザ情報を読み出し送信する。

【0032】主装置301は、データキャリア装置303から返送された個別ユーザ情報が登録された情報と一致することを確認し(S6)、仮に異なっていた場合、再度前記同様の手順により再登録動作を行う。

【0033】以上の一連の登録動作を行った主装置301は、最後に登録ユーザに対し、最大登録ユーザ数の確認を行い、この値が1であった場合、既に登録されたユーザ以外の登録動作を禁止し、登録動作を終了する。

【0034】なお、以上の登録動作においては、主装置識別コードは1つとなっているが、この識別コードにさらに番号等を付加することにより、複数の個別ユーザ情報を組み込むことが可能となり、例えばコンピュータの起動を行うための個別ユーザ情報と、ネットワーク接続のための個別ユーザ情報を分けて登録することも可能である。

【0035】次に、実際のセキュリティ動作について図5に基づき説明する。なお、図5は動作の概略を示すものであり、詳細は省略している。

【0036】まず、主装置301の電源が投入されると、初期立ち上げ動作後(S11)、主装置301はユーザ確認動作に移行し、前記登録動作に含まれるユーザ照合と同様、照合要求データを送出する(S12)。この信号を受信したデータキャリア303は、信号解析した後、個別ユーザ情報部203に書き込まれているデータを返送する。

【0037】この返送データを受信した主装置301は(S13)、個別ユーザ情報に含まれる登録されたユニークな情報の照合を行い(S14)、一致していた場合、次いで同エリア203に含まれる使用履歴情報と、主装置301で保存している履歴情報の一致を確認し

6

(S15)、履歴が一致した場合、データキャリア装置303に対して新しい履歴を送出するとともに、主装置の履歴も更新した後(S17)、プログラムの立ち上げ動作へと移行する(S18)。

【0038】この履歴情報を受けたデータキャリア装置303は、このデータをメモリ104内の個別ユーザ情報部203に書き込み次の要求が来るまで保存する。

【0039】仮に、ユーザ照合において不一致となった場合、主装置301は起動停止メッセージを表示した後(S19)、プログラム起動動作を中断し、再度電源投入もしくは、コンピュータのリセットが行われるまで動作を停止し(S20)、この動作が行われた場合、再度上記動作を繰り返す。

【0040】また、ユーザ照合が一致し、使用履歴が一致しない場合は、ユーザに対し履歴不一致情報を通知した後(S21)、プログラム起動動作へと移行し、セキュリティ動作を完了する。

【第2実施例】以下、本発明の第2実施例として、上述した第1実施例で示したセキュリティシステムをネットワークに接続した場合の応用例について説明する。

【0041】まず図6は、本実施例のセキュリティシステムをネットワークに接続されたシステム応用した場合の接続図であり、図7、図8は、このセキュリティシステムにおける実際の動作を示すフローチャートである。

【0042】図6において、コンピュータ501は、第1実施例の主装置と同様の機能を有するコンピュータ端末(以下端末という)であり、コンピュータ502は、コンピュータ501にLAN503により接続されたネットワークサーバ(以下サーバという)である。

【0043】各端末501は、それぞれデータキャリア装置504との通信機能を有する。また、本実施例において、サーバ502ではデータキャリア装置について記載していないが、このサーバ502にも同様の機能をもたせることは可能であり、この場合、サーバ管理者のみが同様のデータキャリア装置をもつこととなる。

【0044】以下にネットワークに応用した場合の動作について具体的に説明する。なお、端末における個別ユーザ情報登録手順については、第1実施例と同様であることから説明は省略する。

【0045】サーバ502では、まずネットワークにアクセス権を与える端末501の登録を行い、その後、本発明を実施するために個別ユーザ情報登録動作に入る。サーバ502では、個別ユーザ情報登録のため端末501に対し、個別ユーザ情報送信要求を送出し、この信号を受けた端末501では、端末操作ユーザが登録されたユーザであることを確認するために、第1実施例と同様のユーザ照合動作を行った後、サーバ502に対して個別ユーザ情報を送出する。この個別ユーザ情報を受けたサーバ502は、次いでやはり第1実施例の登録動作同様、登録された個別ユーザ情報が正しいかどうかを確認

するためにネットワークを通して端末501に、ユーザ照合要求を出力し、その応答が一致した時点でユーザ登録動作を完了する。

【0046】ユーザ登録動作を完了したサーバ管理者は、この登録されたユーザに対し、アクセス権を与えるデータベース、プログラム等に個別に個別ユーザ情報登録を行うことで、各ユーザに併せてアクセス権の割り当てを行うことができる。

【0047】次に具体的なサーバ502への接続動作時について図7、図8のフローチャートに基づき説明する。なお、図7は端末501の動作を示し、図8はサーバ502の動作を示している。

【0048】サーバ502に接続しようとする端末501は、ネットワーク接続手順を行い(S31)、サーバ502とのコネクションを確立する(S32、S33)。

【0049】一方、コネクション要求を端末501から受けたサーバ502は(S51)、端末501に対し、ユーザ照合要求を送出する(S52)。この要求信号を受信した端末501は(S32)、データキャリア装置504に対し、ユーザ照合電波の送出行い(S34)、データキャリア装置504から返送された照合データおよび履歴データをネットワークを通してサーバ502に送出的(S35、S36)。

【0050】なお、仮にデータキャリア装置504からユーザ情報が受信されなかった場合、アクセス拒否メッセージ表示を行った後(S41)、サーバ502との切断動作を行い(S43)、動作を終了する。

【0051】端末501からユーザ照合データを受信したサーバ502は(S53、S54)、前述した登録動作により登録された個別ユーザ情報との照合を行い(S55)、一致した場合(S56)、照合一致応答を送出し(S57)、次いで最終使用履歴の照合を行い(S58)、一致した場合は履歴の更新情報を(S62)、一致しない場合は履歴不一致情報を(S61)、端末501に送出した後、端末接続許可を出し(S63)、端末の接続動作を完了する。

【0052】仮にユーザ情報が不一致の場合は、端末501に対してアクセス拒否応答を送出し(S59)、切断を行った後(S60)、接続動作を終了する。

【0053】一方、照合一致信号を受信した端末501は(S37)、次いでサーバ同様、最終使用履歴の照合を行い(S38)、一致した場合は履歴の更新を送出し(S40)、不一致の場合は不一致メッセージを送出し、警告表示を行う(S39)。その後、サーバ接続を行い(S42)、接続動作を完了する。

【0054】また、S37でサーバ502からアクセス拒否応答を受信した場合は、同メッセージを表示した後(S41)、ネットワークの切断を行った後(S43)、接続動作を完了する。

【0055】なお、以上の説明においては、初めのコネクション確立のみを説明しているが、サーバの登録動作で説明したように、個別のデータベース等にも同様のセキュリティがかけられることから、この場合においては、アクセス要求があるたびに前述と同様の照合動作が行われる。

【0056】また、本実施例では、サーバ502に個別ユーザ情報を登録する方法を記載しているが、この情報は端末501のみに登録し、接続するサーバ502に応じて照合動作を行い、登録されていないサーバへはアクセス動作を禁止する方法も可能である。

【0057】また、ユーザ照合動作に関しても、本実施例ではサーバ502にて行う方法で説明しているが、ユーザ照合は端末501において行い、照合結果のみをサーバ502に通知する方法でも同様の効果が得られる。

【第3実施例】次に本発明を自動車のセキュリティに応用した場合について説明する。

【0058】図9は、本発明を実施した自動車の計器板とハンドルの周辺部の様子を示す正面図であり、図10は、同システムにおける主装置の動作を示すフローチャートである。

【0059】図9において、計器板700の隅部に主装置701が設けられ、キー703にキーホルダ状のデータキャリア装置702が設けられている。

【0060】このデータキャリア装置702における個別ユーザ情報は、このシステムを出荷するときに、予め主装置701とデータキャリア装置702に登録されているものとする。ただし、この登録手段については、この限りではなく、特殊手段を用いてユーザに開放し、適宜設定できるようにすることも可能である。

【0061】次に、具体的な動作についてフローチャートに基づき説明する。

【0062】まず自動車を使うユーザは、鍵を車に装着し、電源スイッチをオンにする。すると、主装置701では、初期立ち上げ動作を行った後(S71)、ユーザ照合電波の送出行い(S72)。この電波を受けたデータキャリア装置702は、第1実施例と同様に、登録された個別ユーザ情報を主装置701に返送する。

【0063】主装置701においては、返送された個別ユーザ情報の照合を行い(S73)、一致した場合(S74)、エンジン始動要求を待機し(S75)、要求があった場合、エンジンの始動を行わない(S76)、動作を完了する。

【0064】また、データキャリア装置702からの応答が受けられない場合、もしくはユーザ照合の結果、不一致の場合は、強制的に電源を切断し(S77)、その動作を終了する。

【0065】本実施例では、エンジン始動のセキュリティにのみデータキャリア装置702を使用しているが、第1実施例で示すようにデータキャリア装置内のメモリ

9

104の個別ユーザ情報部203に履歴等を残すことが可能であることから、例えば車のシステム管理データに異常値が発生した場合、このデータをデータキャリア装置702に転送し、保存することも可能である。

【0066】

【発明の効果】以上説明したように、本発明によれば、例えばコンピュータのセキュリティに用いる場合、データキャリア装置に個別ユーザ情報および最終使用履歴を保存する保存手段と、照合要求があった場合、蓄積されたデータを主装置に返送する返送手段を有することにより、OS等のもつパスワードによる保護に加え、使用者を登録されたデータキャリア装置をもつユーザのみに特定でき、より信頼性の高いセキュリティが確保できる。

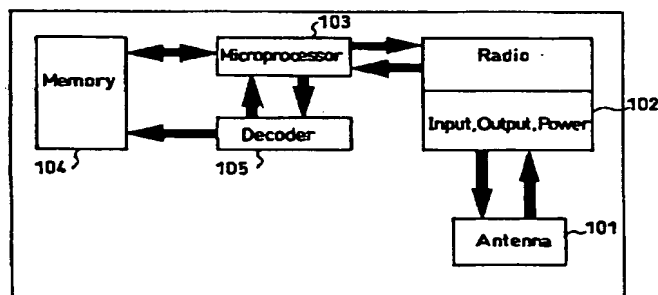
【0067】また、さらに最終使用履歴を主装置およびデータキャリア装置でそれぞれ有し、照合時に互いのデータに違いがないことを確認する確認手段を有することにより、仮にデータキャリア装置を不正に複製された場合においても、ユーザがコンピュータの不正使用されたことを知ることが可能となり、容易に個別ユーザ情報の変更等による対策が行える。

【0068】また、自動車のセキュリティに用いた場合においては、常にエンジン始動時に照合動作が行われることから、ユーザは意識することなく常に盗難防止機能がかけられる。

【0069】さらに、主装置の識別コードを伝送データに組み込むことで、入退室管理システム等、複数のシステムを1つのデータキャリア装置で共用することが可能となり、ユーザは意識することなく複数のシステムを使用できる。

【0070】また、以上のような構成を用いることによ

【図1】



10

*り、システム全体の消費電力を大幅に削減することが可能となり、バッテリー駆動の機器にも容易に用いることができる。

【図面の簡単な説明】

【図1】本発明の実施例におけるデータキャリア装置の内部構成を示すブロック図である。

【図2】上記実施例におけるデータフォーマットを示す説明図である。

【図3】上記実施例によるシステムを構成する機器の外観を示す説明図である。

【図4】本発明の第1実施例の動作を示すフローチャートである。

【図5】上記第1実施例の動作を示すフローチャートである。

【図6】本発明の第2実施例によるネットワークシステムの概要を示す説明図である。

【図7】上記第2実施例の動作を示すフローチャートである。

【図8】上記第2実施例の動作を示すフローチャートである。

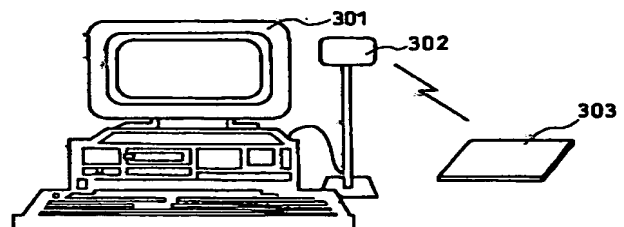
【図9】本発明の第3実施例によるシステムを構成する機器の外観を示す説明図である。

【図10】上記第3実施例の動作を示すフローチャートである。

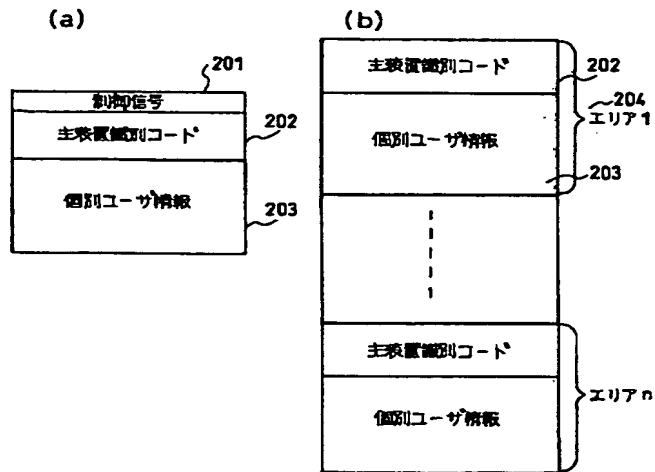
【符号の説明】

- 101…アンテナ、
- 102…無線部、
- 103…プロセッサ、
- 104…メモリ、
- 105…デコーダ。

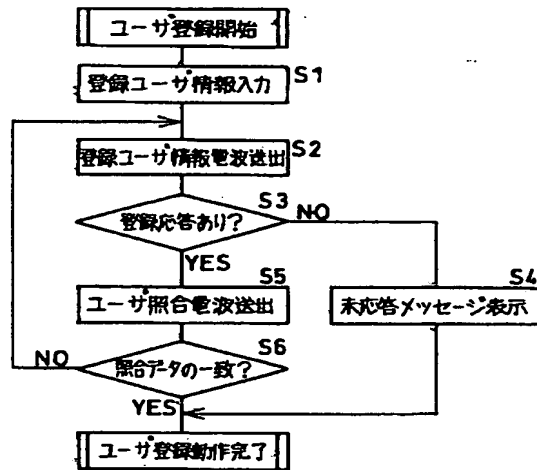
【図3】



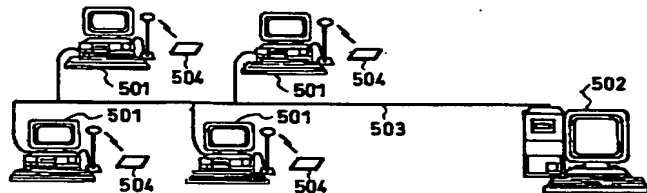
【図2】



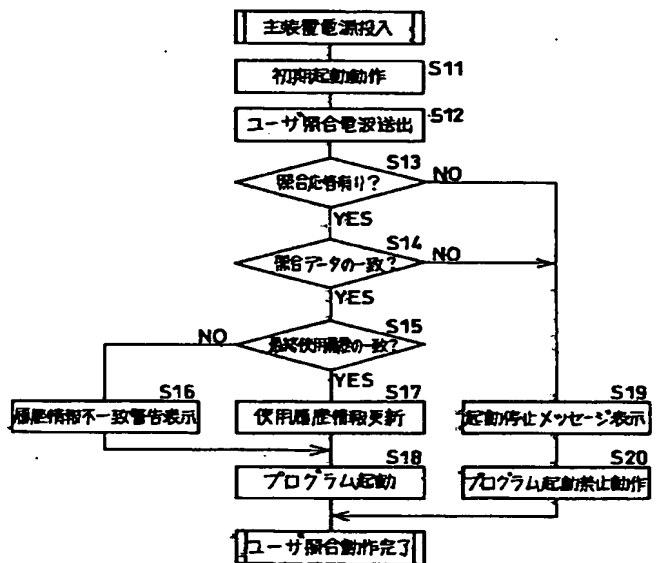
【図4】



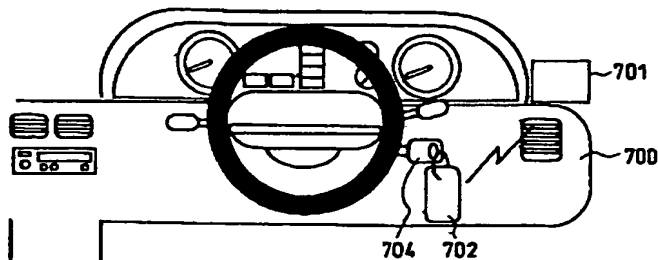
【図5】



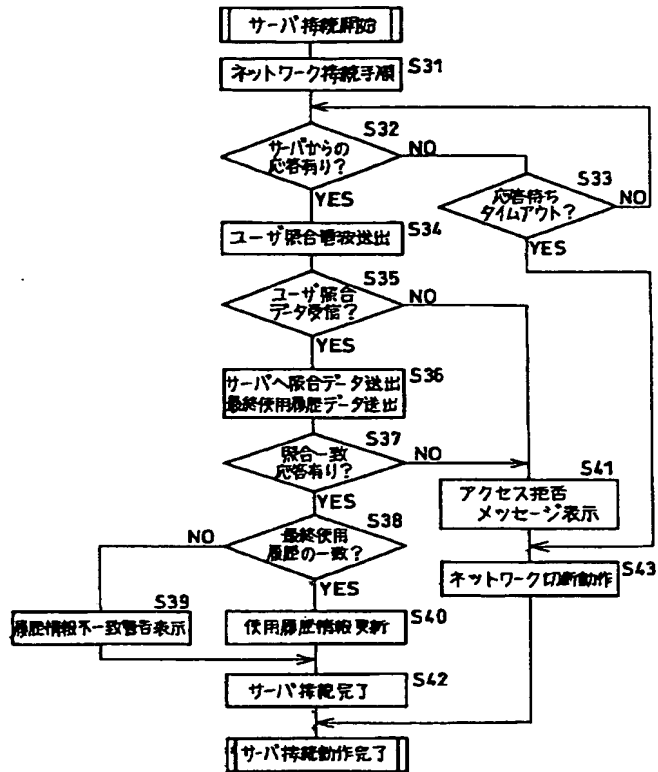
【図6】



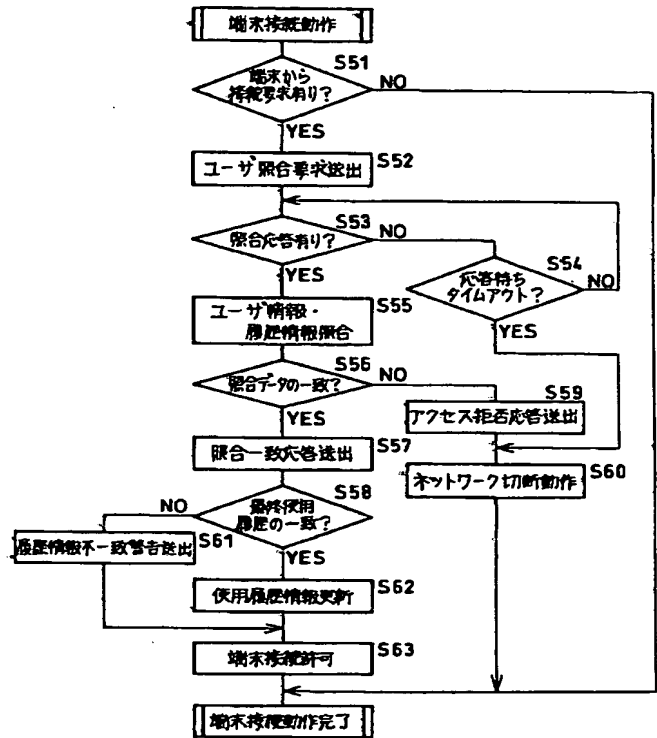
【図9】



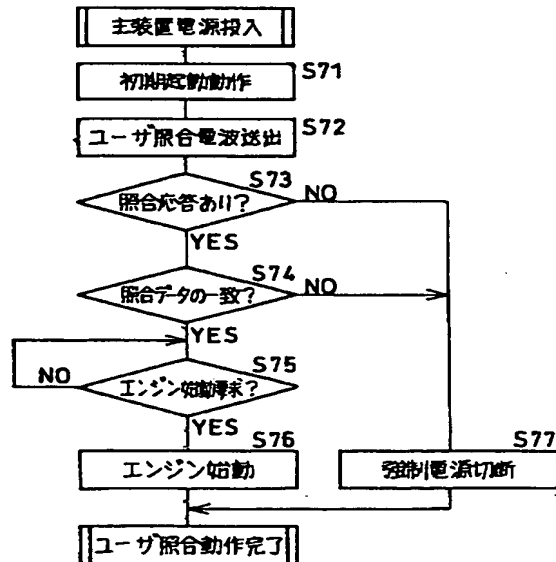
【図 7】



【図 8】



【図 10】



フロントページの続き

(51)Int.Cl. 7

識別記号

F I
H 0 4 L 9/00

テーマコード(参考)

6 7 3 B